Set Task Electronic Template – Unit 11

Task B - Activity 4 Template: Forensic Incident Analysis

*Use the section headings below to structure a response for **each** evidence item.*

Evidence item: 1 Baljinder's account

Method of acquiring the evidence: Conversation with Baljinder

Evidence detail: Baljinder's account is based on recollection and what he had saw. It gives an approximate timeline of the sequence of events.

Evidence reliability: The reliability is fair. Baljinder is likely to be telling the truth, however relying upon a person's memory wouldn't produce perfect results and Baljinder could have made a mistake or forgotten some detail.

Conclusions: The laptop and the phone supposedly went missing over the May bank holiday. The place was empty by 14:00 on Friday lunchtime where between then and Tuesday morning, the things in question went missing. With such a broad timeline, its not easy to pinpoint the exact time the items went missing. The Samsung Edge S5 phone and the Surface Pro 3 laptop were charging on one of the tables in the informal seating area which can accessed by anyone with access to the space behind the controlled doors. The police were unable to do much since there was no forced entry but gave Baljinder an incident number for insurance purposes. The phone was blocked and tracked on the 3rd April to a district named Nairobi but since then no further reports were received. Also, the files on the laptop had been copied to the file server at the end of the meeting – there was no confidential information, just a report regarding use of fire extinguishers.

Evidence item: 2 Summary of a meeting with the Edexcelsior House management company

Method of acquiring the evidence: Notes form a meeting with the senior management on the Wednesday after the incident.

Evidence detail: The EH company said there had been a few incidents over the Bank Holiday weekend, so Baljinder met with them to discuss the events. They met on Wednesday after the incident. The people present were representatives from the EH management company, restaurant and bar, ground floor shops, the recruitment agency from the 18th floor.

Evidence reliability: Good. The reliability is good as it would information very close on what was said. Although, some mistakes could have been made or some information could have been missed out when scribing.

Conclusions: In the meeting there was an assurance that maintenance and cleaners were not responsible as they are paid a high wage, in the history of the company's existence there have been few dismissals for dishonesty, none this year and loyalty being good. This kind of takes the cleaning and maintenance staff out of the list of 'suspects'. This also makes sense since there has also been pickpocketing and opportunity thefts Friday evening. The levels of theft were at an all-time high on Friday but returned back to its normal low level for the rest of the weekend. This may indicate that the thefts of equipment, pickpocketing and BCTAA may have happened

on Friday afternoon/ evening. The shops also reported problems with customers having phantom charges applied to some contactless payment cards. This indicates that the same thieves could have operated the same events and be specialists in IT

Evidence item: 3 Door access control logs

Method of acquiring evidence: All the doors are controlled through a networked system, using near field communication/proximity cards, similar to those used for contactless payment systems. The EH management company supplies cards, a card programming device and logging and control software.

Evidence detail: The logs show the card numbers associated with the group/ person so those who are on floor 19 have a card number beginning with 19, the EH company uses cards beginning with the number 99 and BCTAA uses cards beginning with 19 since they're on the 19th floor. Access via 99 cards is logged on the BCTAA system and also sent via a network link to the management company where it is checked against scheduled access.

Evidence reliability: Good. The software records those who scanned their cards in and out according to their card information. The system shows access dates and times, the card numbers used and when they come in and out. It also shows unscheduled access and the differences in card numbers.

Conclusions: The last group leaving after work was let out by the person with card 26 at 13:42 where all the offices were checked and left empty o the 30th march. This means that nobody could have been left in the office to carry out this incident, especially since scheduled cleaning staff went in to clean the offices. There was also a security check at 22:18 for 2 minutes and another on the morning of the 31st of March. Access by thieves between these times is unlikely, especially since regarding the report there was no forced entry, so a card must have been used. In the logs, there is no sign of suspicious activity until the 31st March at 23:31 where a card was used to gain access during a party on the 20th floor. There was also a correct card for floor 18 which was used and another card at 23:32. All deny that they used the card and one stated that he wasn't sure as he couldn't remember. A senior management card was used at 23:32 the same night but the card holder says that they were at a party on the 20th floor all night. So if the card holders didn't use their cards that night, that means that someone has either stolen their cards or duplicated them with the same information to impersonate the holder.

Evidence item: 4, Network diagram

Method of acquiring evidence: This would be part of the document for the current system and network layout.

Evidence detail: The diagram shows connections between the electronic door control system and the contactless cards to the main switch, WiFi router, servers and optical fibre internet access point.

Evidence reliability: Good, there is no evidence to suggest that the diagram has been altered.

Conclusions: Looking at the network diagram, it is possible that the thief/ thieves may

have gained access to the key card information through their mobile device via the internet. This would mean that the intruder could copy key card information to gain access to the offices and private rooms where they could steal the items. Although, a Wi-Fi intrusion would be likely to infect computers on the system and trigger an alert.

Evidence item: 5, Laptop tracking report

Method of acquiring evidence: 'Find my device' is a software on the laptop which can pin point its location from another device when its connected to internet.

Evidence detail: The report shows that there was one result which shown the laptop to be in Nairobi, Kenya on the 09/04/2018. After this there was no further result received.

Evidence reliability: Good, this is because the 'find my device' application uses an external GPS system which more than likely will give the correct location of the device.

Conclusions: Since the only result shows the laptop to be/ was in Kenya, the person who stole the laptop is likely to of either travelled with the laptop or sent it via post there to be cleaned and wiped / sold. This means the laptop is unlikely to be retrieved.

Overall Conclusion:

In conclusion, the evidence shows that someone may of had duplicated the cards. It is fair that the reason that Baljindier said he is not very sure of the time all items went missing but he was sure it happened over the bank holiday weekend. This is backed up by the door access log. Although, someone could have stolen the cards from those who are at the party but the likely outcome is someone duplicated the cards the first three didn't allow them entry being the card number ending in 0035,00775,00029, so they duplicated the senior manager's card ending in 00010. In addition, a summary of the meeting with the EH management company noted that there were many cases of pickpocketing that occurred meaning cards may have been stolen at that time. Another thing mentioned in the meeting was phantom charges that occurred on contactless payments which could mean that the same system used to duplicate the contactless cards was used to charge contactless payments and cause phantom charges. Finally, the card whose holder was a senior manager of BCTAA 0010 was the only card which worked at the that time of access, so the person/ people trying to enter must not belong to BCTAA as they'd know that any cards of regular employees is restricted at that time of the day.